

# Explore the Future of Third-Party Risk Management with AI and Beyond

Opportunities and Challenges October 4, 2023



The information herein has been provided by CliftonLarsonAllen LLP for general information purposes only. The presentation and related materials, if any, do not implicate any client, advisory, fiduciary, or professional relationship between you and CliftonLarsonAllen LLP and neither CliftonLarsonAllen LLP nor any other person or entity is, in connection with the presentation and/or materials, engaged in rendering auditing, accounting, tax, legal, medical, investment, advisory, consulting, or any other professional service or advice. Neither the presentation nor the materials, if any, should be considered a substitute for your independent investigation and your sound technical business judgment. You or your entity, if applicable, should consult with a professional advisor familiar with your particular factual situation for advice or service concerning any specific matters.

CliftonLarsonAllen LLP is not licensed to practice law, nor does it practice law. The presentation and materials, if any, are for general guidance purposes and not a substitute for compliance obligations. The presentation and/or materials may not be applicable to, or suitable for, your specific circumstances or needs, and may require consultation with counsel, consultants, or advisors if any action is to be contemplated. You should contact your CliftonLarsonAllen LLP or other professional prior to taking any action based upon the information in the presentation or materials provided. CliftonLarsonAllen LLP assumes no obligation to inform you of any changes in laws or other factors that could affect the information contained herein.

# At the end of this session, you will be able to:

- Identify the opportunities AI presents to organizations
- Discuss the key cybersecurity risks of Al
- Recall different types of Al-powered cyberattack





## What is Artificial Intelligence?

- Systems that exhibit intelligence as defined by humans
- Complex tasks
- Machine learning
- Deep learning
- Mimic human cognition





#### Where is this Going?

#### Moore's Law

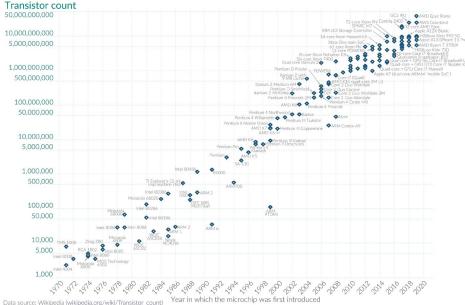
Geometric Growth

**Getting Better Faster** 

#### Moore's Law: The number of transistors on microchips doubles every two years Our World

Moore's law describes the empirical regularity that the number of transistors on integrated circuits doubles approximately every two years. This advancement is important for other aspects of technological progress in computing – such as processing speed or the price of computers.





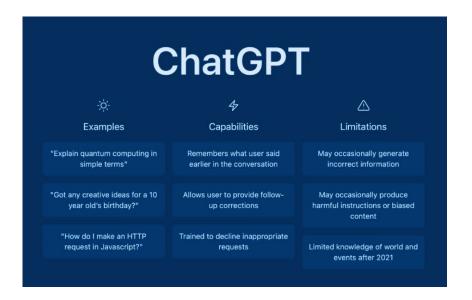
Our Worldin Data, org – Research and data to make progress against the world's largest problems. Licensed under CC-BY by the authors Hannah Ritchie and Max Roser.





#### ChatGPT

- Predict the next word
- Human centered feedback
- Other secret sauce?







## Use Cases

Demo





# Agents







**PLANNING** 



**OBJECTIVE BASED** 





#### Risk Debate

#### Geoffery Hinton

'Right now there are 99 very smart people trying to make AI better and one very smart person trying to figure out how to stop it taking over and maybe you want to be more balanced'

'So, there's the alignment worry that we give it a perfectly reasonable goal, and it decides that, well, in order to achieve that, I'm going to get — get myself a lot more power. And because it's much smarter than us, and because it's trained from everything people ever do this — it's read every novel that ever was, it's read Machiavelli, it knows a lot about how to manipulate people — there's the worry that it might start manipulating us into giving it more power, and we might not have a clue what's going on.'

'Godfather Of AI' Urges Governments To Stop Machine Takeover | Barron's (barrons.com)

'Godfather of AI' discusses dangers the developing technologies pose to society | PBS NewsHour

#### Yann LeCun

'Al is an amplifier of human intelligence & when people are smarter, better things happen: people are more productive, happier & the economy strives.'

'A fear that has been popularized by science fictions [is], that if robots are smarter than us, they are going to want to take over the world ... there is no correlation between being smart and wanting to take over'

'[AI is] missing something really big ... to reach not just human level intelligence, but even dog intelligence'

https://x.com/ylecun/status/1671926268122611727?s=20





#### The Cybersecurity Conundrum

# Cybercriminals can Utilize Free/Cheap Al Services

- Empowers criminals to quickly create sophisticated attacks
- Al tools that construct malicious code and convincing deep fakes

# Al Benefits Enterprises more than Criminals, however:

- There's a high cost and skill requirement to maintain these benefits
- 82% of Data Breaches are still the result of human error





#### Deep Fakes

- Al Trained to fool
  - Mimic a CEO's Voice
  - Spread Misinformation as Famous Figures
- Will continue to get worse
- Arms race





#### AI-Powered Malware/Ransomware

- Ransomware remains one of the biggest cyber threats
  - Ex: MGM Casino
- WormGPT Al model trained in malware creation
- Al Models like these:
  - Increases the speed of attacks
  - Increases attack success
  - Decreases required expertise
  - Decreases necessary cost





#### Prompt Injections/Data Poisoning

- Prompt Injection Using Prompts to force an AI to ignore its guard rails and perform unintended actions
  - Possibility to leak sensitive information
  - Lacks simple mitigation
- Data Poisoning Purposefully introducing malicious data into training data for an AI model
  - Leads to bias or inaccurate results
  - Risk to organizations developing internal AI models





#### Managing AI Risk

- All users have a responsibility to verify Al output
  - "It's a mistake to be relying on [AI] for anything important right now"
     Sam Altman, CEO of OpenAI
- Include AI in acceptable use policies
  - Rules for safe and ethical AI usage
- Appoint lead/group focused on navigating AI decisions
- NIST AI risk management framework





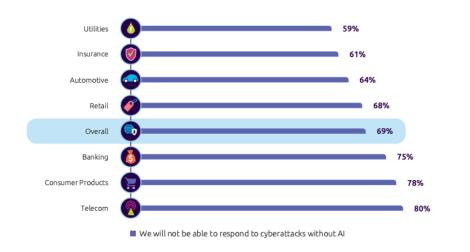
## Need for AI in Cybersecurity

 56% of cybersecurity teams are overwhelmed

- Security issues cannot be remediated quickly
  - Likelihood of breaches increase

 35% of businesses faced attacks on critical operations

Figure 1: Organizations are counting on AI to help identify threats and thwart attacks







#### Benefits of AI to Cybersecurity

- Ability to analyze large amounts of data
  - Enhances threat hunting & incident response
  - Reduces time spent analyzing logs
- Monitoring and pattern recognition
- Reduces the risk of human error





#### AI Overcoming Threats

#### Proactive Network Defense

- AI identification of normal & malicious network activity
- 90% Malware detection accuracy
- Ability to detect rare forms of malware

#### **Email Monitoring**

- Filter/flags potential phishing emails
- Reduces potential of human error
- Past emails reused for enhancing recognition

### Intelligence Gathering

- Analyze data from external sources
- Keeps security team informed of cyber threats









# Any Questions?

©2023 CliftonLarsonAllen LLP. CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See CLAglobal.com/disclaimer. Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.



#### Thank you for joining us!

**Lindsay Timcke** 

Signing Director
<a href="mailto:lindsay.timcke@CLAconnect.com">lindsay.timcke@CLAconnect.com</a>
781-610-1249

**Liam McGoldrick** 

Data Scientist Manager
<a href="mailto:liam.mcgoldrick@CLAconnect.com">liam.mcgoldrick@CLAconnect.com</a>
813-739-7604

**Robert Johnson** Director, Digital Growth Robert.johnson@CLAconnect.com 571-227-9584

©2023 CliftonLarsonAllen LLP. CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See CLAglobal.com/disclaimer. Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.

## References/Sources

- What is Artificial Intelligence (AI) ? | IBM
- Al-Powered Phishing: Attacker vs. Defender Who Prevails | LinkedIn
- The Promise and Peril of the Al Revolution: Managing Risk | ISACA
- Reinventing Cybersecurity with Artificial Intelligence | Capgemini



